EXHIBIT 2

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/403,818	03/31/2003	Hasan S. Alkhatib	INNF0017	2698

75671 7590 02/04/2009

Sadler, Breen, Morasch & Colby, ps
422 W. Riverside Ave, Suite 424
Spokane, WA 99201

EXAMINER	
BLAIR, DOUGLAS B	
ART UNIT	PAPER NUMBER
2442	
MAIL DATE	DELIVERY MODE
02/04/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/403,818	ALKHATIB ET AL.	
	Examiner	Art Unit	
	DOUGLAS B. BLAIR	2442	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 March 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-24,26-36,41-44,53-66,68-100 and 102-109* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-24,26-36,41-44,53-66,68-100 and 102-109* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *12/5/07,8/21/08, 10/21/08* .
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 3/14/2008 has been entered.

Response to Arguments

Applicant's arguments with respect to claims 1-24, 26-36, 41-44, 53-66, 68-100, and 102-109 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 1-24, 26-36, 41-44, 53-66, 68-79, 93-100, and 102-109 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claims 1-24 and 26-31 are directed towards a virtual network system comprising a virtual network manager and a route director. Because these elements are disclosed as possibly being software elements they are treated as software per se. Claims 32-36, 41-44, 93-100, and 102-109 are directed towards the virtual network manager. Claims 53-63 are directed towards a system

comprising a virtual network manager, a route director, and software agents. Software per se does not fit into a statutory category of invention.

Claims 64-66 and 68-79 are rejected under 35 U.S.C. 101 as not falling within one of the four statutory categories of invention. While the claims recite a series of steps or acts to be performed, a statutory "process" under 35 U.S.C. 101 must (1) be tied to particular machine, or (2) transform underlying subject matter (such as an article or material) to a different state or thing. See page 10 of In Re Bilski 88 USPQ2d 1385. The instant claims are neither positively tied to a particular machine that accomplishes the claimed method steps nor transform underlying subject matter, and therefore do not qualify as a statutory process.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-15, 17-24, 26, 29-43, 53-56, 59, 60-66, 68-87, 90-100, and 102-109 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent Application Publication Number 2008/0232295 by Kreiner et al.

As to claim 1, Kreiner teaches a virtual network system, comprising: a virtual network manager configured to register devices in a virtual network that is defined by a domain name (paragraph 39), each device in the virtual network being identified to the other devices by a virtual network

address that is unique for each device and not directly routable via a public network, the virtual network manager further configured to distribute a virtual network address to a device when the device is registered in the virtual network (paragraph 35); and a route director configured to communicate data between the devices that are registered in the virtual network, the data being communicated as encapsulated packets from a source device to a destination device, an encapsulated packet including a first virtual network address that corresponds to the source device and a second virtual network address that corresponds to the destination device (paragraph 38).

As to claim 2, Kreiner teaches the system of claim 1 wherein each of the devices communicate with the virtual network manager and the other devices in the virtual network via an associated agent (paragraphs 30-39).

As to claim 3, Kreiner teaches the system of claim 1 wherein each of the devices include an agent configured to communicate with the virtual network manager and agents of the other devices in the virtual network (paragraphs 30-39).

As to claim 4, Kreiner teaches the system of claim 2 wherein the associated agent is installed on a proxy device which is a proxy agent for one or more of the devices in the virtual network with respect to the virtual network manager and the route director (Figure 2, personal gateway).

As to claim 5, Kreiner teaches the system of claim 2 wherein the virtual network manager is further configured to: receive a request from the agent associated with a device in a private network to register the device in the virtual network; and detect a presence of a NAT device via which the request is routed from the agent to the virtual network manager (paragraphs 30-39).

As to claim 6, Kreiner teaches the system of claim 1 wherein the virtual network manager is

coupled to the public network and has an associated public network address (paragraphs 30-39).

As to claim 7, Kreiner teaches the system of claim 1 wherein the route director is further configured to receive the encapsulated packets when routed to a public network address corresponding to the route director (paragraphs 30-39).

As to claim 8, Kreiner teaches the system of claim 1 wherein each of the devices in the virtual network are further identified by at least one physical network address (paragraphs 30-39).

As to claim 9, Kreiner teaches the system of claim 8 wherein the physical network addresses that are associated with the devices in the virtual network are dynamic (paragraphs 30-39).

As to claim 10, Kreiner teaches the system of claim 8 wherein the physical network addresses that are associated with the devices in the virtual network are static (paragraphs 30-39).

As to claim 11, Kreiner teaches the system of claim 8 wherein the physical network addresses that are associated with the devices in the virtual network are private network addresses, and wherein the virtual network addresses are unique in the virtual network so as not to conflict with the private network addresses (paragraphs 30-39).

As to claim 12, Kreiner teaches the system of claim 8 wherein the source device is coupled to a first private network and accesses a public network via a first NAT device configured to transmit the encapsulated packets, an encapsulated packet further including the physical network address of the source device as a private network address in the first private network (paragraphs 30-39).

As to claim 13, Kreiner teaches the system of claim 12 wherein the physical network address of the source device is dynamic (paragraphs 30-39).

As to claim 14, Kreiner teaches the system of claim 12 wherein the physical network address of the source device is static (paragraphs 30-39).

As to claim 15, Kreiner teaches the system of claim 12 wherein the destination device is coupled to a second private network and accesses the public network via a second NAT device, the encapsulated packet further including the physical network address of the destination device as a private network address in the second private network (paragraphs 30-39).

As to claim 17, Kreiner teaches the system of claim 15 wherein the physical network address of the destination device is dynamic (paragraphs 30-39).

As to claim 18, Kreiner teaches the system of claim 15 wherein the physical network address of the destination device is static (paragraphs 30-39).

As to claim 19, Kreiner teaches the system of claim 15 wherein said first private network and said second private network share at least one network address (paragraphs 30-39).

As to claim 20, Kreiner teaches the system of claim 1 wherein the route director is further configured to: provide a device-specific pseudo address assignment for the device in the virtual network when the device communicates with the route director via a NAT device; and store an association of the device-specific pseudo address with a public network address of the NAT device and a port number of the NAT device (paragraphs 30-39).

As to claim 21, Kreiner teaches the system of claim 1 wherein the route director includes a translator for virtual network address information for a device in the virtual network that is implemented in a private network (paragraphs 30-39).

As to claim 22, Kreiner teaches the system of claim 1 wherein the virtual network manager is coupled to the public network and includes a public network address (paragraphs 30-39).

As to claim 23, Kreiner teaches the system of claim 22 wherein the route director is coupled to the public network and includes a different public network address than the public network address of the virtual network manager (paragraphs 30-39).

As to claim 24, Kreiner teaches the system of claim 22 wherein the route director is coupled to a private network and includes a private network address (paragraphs 30-39).

As to claim 26, Kreiner teaches the system of claim 1 wherein the encapsulated packets further include virtual IP packets configured for communication of the data, the virtual IP packets being encrypted prior to being encapsulated (paragraphs 30-39).

As to claim 29, Kreiner teaches the system of claim 5 wherein the virtual network manager is further configured to receive the request from the agent as a message, and detect the presence of the NAT device by comparing a field in a payload of the message with a source address in a header of the message (paragraphs 30-39).

As to claim 30, Kreiner teaches the system of claim 1 wherein the virtual network manager includes a virtual community definition that is defined by the domain name, and includes one or more of the devices that are registered in the virtual network (paragraphs 30-39).

As to claim 31, Kreiner teaches the system of claim 1 wherein the route director is a public route director in the public network, the system further comprising a private route director in a private network configured to enable access to devices of the private network that are also in

the virtual network from devices of the public network that are also in the virtual network (paragraphs 30-39).

As to the rest of the claims they are rejected for the same reasons.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 27 and 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent Application Publication Number 2008/0232295 by Kreiner et al.

As to claims 27-28, official notice is taken that the claimed types of encryption are well known and the applicant has not disclosed anything novel related to them so they are not themselves patentable.

Allowable Subject Matter

Claims 16 and 44 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

The following is a statement of reasons for the indication of allowable subject matter: The prior art does not teach he claimed relation between the elements claimed.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to DOUGLAS B. BLAIR whose telephone number is (571)272-3893. The examiner can normally be reached on 9:00am-5:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Douglas B Blair/
Primary Examiner, Art Unit 2442

LIST OF CLAIMS / AMENDMENTS

Claims 25, 37-40, 45-52, 67, and 101 were previously canceled.

Please cancel claims 16 and 44 without prejudice.

Please amend claims 1, 32, 53, 57, 58, 64, 80, 81, 83, 85-87, 92, and 93 as shown herein.

Claims 1-15, 17-24, 26-36, 41-43, 53-66, 68-100, and 102-109 are pending:

1. (currently amended) A virtual network system, comprising:

a virtual network manager implemented as a first computing device, the virtual network manager configured to register devices in a virtual network that is defined by a domain name, each device in the virtual network being identified to the other devices by a virtual network address that is unique for each device and not directly routable via a public network, the virtual network manager further configured to distribute a virtual network address to a device when the device is registered in the virtual network; ~~and~~

a route director implemented as a second computing device, the route director configured to communicate data between the devices that are registered in the virtual network, the data being communicated as encapsulated packets from a source device to a destination device, an encapsulated packet including a first virtual network address that corresponds to the source device and a second virtual network address that corresponds to the destination device; and

the virtual network manager further configured to receive a DNS request from the source device, and return a public network address of the route director, a private network address for the destination device, and the second virtual network address that corresponds to the destination device.

2. (previously presented) The system of claim 1 wherein each of the devices communicate with the virtual network manager and the other devices in the virtual network via an associated agent.

3. (previously presented) The system of claim 1 wherein each of the devices include an agent configured to communicate with the virtual network manager and agents of the other devices in the virtual network.

4. (previously presented) The system of claim 2 wherein the associated agent is installed on a proxy device which is a proxy agent for one or more of the devices in the virtual network with respect to the virtual network manager and the route director.

5. (previously presented) The system of claim 2 wherein the virtual network manager is further configured to:

receive a request from the agent associated with a device in a private network to register the device in the virtual network; and

detect a presence of a NAT device via which the request is routed from the agent to the virtual network manager.

6. (previously presented) The system of claim 1 wherein the virtual network manager is coupled to the public network and has an associated public network address.

7. (previously presented) The system of claim 1 wherein the route director is further configured to receive the encapsulated packets when routed to a public network address corresponding to the route director.

8. (previously presented) The system of claim 1 wherein each of the devices in the virtual network are further identified by at least one physical network address.

9. (previously presented) The system of claim 8 wherein the physical network addresses that are associated with the devices in the virtual network are dynamic.

10. (previously presented) The system of claim 8 wherein the physical network addresses that are associated with the devices in the virtual network are static.

11. (previously presented) The system of claim 8 wherein the physical network addresses that are associated with the devices in the virtual network are private network addresses, and wherein the virtual network addresses are unique in the virtual network so as not to conflict with the private network addresses.

12. (previously presented) The system of claim 8 wherein the source device is coupled to a first private network and accesses a public network via a first NAT device configured to transmit the encapsulated packets, an encapsulated packet further including the physical network address of the source device as a private network address in the first private network.

13. (previously presented) The system of claim 12 wherein the physical network address of the source device is dynamic.

14. (previously presented) The system of claim 12 wherein the physical network address of the source device is static.

15. (previously presented) The system of claim 12 wherein the destination device is coupled to a second private network and accesses the public network via a second NAT device, the encapsulated packet further including the physical network address of the destination device as a private network address in the second private network.

16. (canceled)

17. (previously presented) The system of claim 15 wherein the physical network address of the destination device is dynamic.

18. (previously presented) The system of claim 15 wherein the physical network address of the destination device is static.

19. (previously presented) The system of claim 15 wherein said first private network and said second private network share at least one network address.

20. (previously presented) The system of claim 1 wherein the route director is further configured to:

provide a device-specific pseudo address assignment for the device in the virtual network when the device communicates with the route director via a NAT device; and

store an association of the device-specific pseudo address with a public network address of the NAT device and a port number of the NAT device.

21. (previously presented) The system of claim 1 wherein the route director includes a translator for virtual network address information for a device in the virtual network that is implemented in a private network.

22. (previously presented) The system of claim 1 wherein the virtual network manager is coupled to the public network and includes a public network address.

23. (previously presented) The system of claim 22 wherein the route director is coupled to the public network and includes a different public network address than the public network address of the virtual network manager.

24. (previously presented) The system of claim 22 wherein the route director is coupled to a private network and includes a private network address.

25. (canceled)

26. (previously presented) The system of claim 1 wherein the encapsulated packets further include virtual IP packets configured for communication of the data, the virtual IP packets being encrypted prior to being encapsulated.

27. (previously presented) The system of claim 26 wherein the virtual IP packets are encrypted using IPSEC.

28. (previously presented) The system of claim 26 wherein the virtual IP packets are encrypted using DES or triple DES.

29. (previously presented) The system of claim 5 wherein the virtual network manager is further configured to receive the request from the agent as a message, and detect the presence of the NAT device by comparing a field in a payload of the message with a source address in a header of the message.

30. (previously presented) The system of claim 1 wherein the virtual network manager includes a virtual community definition that is defined by the domain name, and includes one or more of the devices that are registered in the virtual network.

31. (previously presented) The system of claim 1 wherein the route director is a public route director in the public network, the system further comprising a private route director in a private network configured to enable access to devices of the private network that are also in the virtual network from devices of the public network that are also in the virtual network.

32. (currently amended) A virtual network manager, comprising:

a network interface configured for data communication via a virtual network that is defined by a domain name having an associated public network address;

a register module configured to register devices in a virtual network, the register module further configured to:

receive a registration request from an agent associated with a device; ~~and~~

distribute a virtual network address to the device when the device is registered in the virtual network, the device being identified to other devices in the virtual network by the virtual network address; and

a DNS server for the virtual network, the DNS server configured to receive a DNS request from a first device in the virtual network, and return a network address associated with a network route director, a private network address associated with a second device in the virtual network, and a virtual network address associated with the second device.

33. (previously presented) The virtual network manager of claim 32 further comprising an additional network interface configured for data communication via a public network.

34. (previously presented) The virtual network manager of claim 32 wherein the network interface is a UDP port configured for data communication via the virtual network.

35. (previously presented) The virtual network manager of claim 33 wherein the network interface is a UDP port configured for data communication via the virtual network, and wherein the additional network interface is a TCP port configured for registration communications via the public network.

36. (previously presented) The virtual network manager of claim 32 wherein the register module is further configured to receive the registration request from the agent that is installed on the device for data communication via the virtual network.

37-40. (canceled)

41. (previously presented) The virtual network manager of claim 32 further comprising a join module configured to receive a join request from the agent associated with the device to indicate that the device is connected for data communication within the virtual network, the join module further configured to receive a leave request from the agent associated with the device to indicate that the device will be disconnected from data communication within the virtual network.

42. (previously presented) The virtual network manager of claim 41 wherein the join module is further configured to provide virtual network addresses to the devices that are registered in the virtual network.

43. (previously presented) The virtual network manager of claim 41 wherein the join module is further configured to maintain data to associate a virtual network address with a device in the virtual network.

44-52. (canceled)

53. (currently amended) A virtual network system, comprising:

a computing device that includes at least a memory and a processor configured to implement a network manager of a virtual network that is defined by a public domain name, the network manager configured to distribute virtual network addresses to devices that register as members in the virtual network, each device in the virtual network being identified to the other devices by a virtual network address associated with the device;

a first virtual network agent associated with a first device that is registered as a member in the virtual network;

at least a second virtual network agent associated with at least a second device that is registered as a member in the virtual network; and

a route director configured to route communications between the first device and the at least second device in the virtual network via the respective first and second virtual network agents, the communications configured for routing as encapsulated packets that include a first virtual network address that is not directly routable corresponding to the first device and a second virtual network address that is not directly routable corresponding to the at least second device.

54. (previously presented) The system of claim 53 wherein the route director is a public network route director that includes a public network interface and an associated public network address by which the first and second virtual network agents communicate with the public network route director.

55. (previously presented) The system of claim 53 wherein the route director is a private route director that includes a private physical network interface and an associated private physical network address.

56. (previously presented) The system of claim 53 wherein the first virtual network agent is installed on the first device for data communication via the virtual network.

57. (currently amended) The system of claim 56 wherein the first device is in a private physical network, has an associated private network address, and has [[an]] the associated virtual network address that is not directly routable ~~and~~ by which the first device can be identified by the at least second virtual network agent from outside of the private physical network.

58. (currently amended) The system of claim 56 wherein the first device is coupled to a public physical network, has an associated public network address, and has [[an]] the associated virtual network address by which the first device can be identified by the at least second virtual network agent.

59. (previously presented) The system of claim 53 wherein the first virtual network agent is a proxy agent for the first device with respect to the network manager and the route director.

60. (previously presented) The system of claim 53 wherein the first and second devices are configured to access the virtual network from separate private address physical realms.

61. (previously presented) The system of claim 53 wherein the network manager includes at least a first community definition and a second community definition, the first community definition being defined by the public domain name and includes one or more of the devices that are registered in the virtual network, and the second community definition being defined by a different public domain name and includes one or more different devices that are registered in the virtual network.

62. (previously presented) The system of claim 53 wherein the network manager includes a member authenticator configured to authenticate the devices that request to register with the network manager.

63. (previously presented) The system of claim 62 wherein the network manager includes a DNS server configured to provide authoritative responses for DNS queries in the virtual network, the DNS server further configured to receive a DNS query from the first device to obtain the virtual network address of the at least second device for use in communicating with the second device.

64. (currently amended) A computer-implemented method, comprising:

receiving registration requests from devices that request to be registered as members of a virtual network that is defined by a domain name having an associated public network address in a public network, each of the devices having an associated private network address; ~~and~~

distributing a virtual network address to a device to register the device as a member in the virtual network, each device in the virtual network being identified to the other devices by the virtual network address that is associated with the device; and

routing communications between the devices that are registered in the virtual network, the communications being routed as encapsulated packets from a source device to a destination device, an encapsulated packet including a first virtual network address that corresponds to the source device and a second virtual network address that corresponds to the destination device.

65. (previously presented) The method of claim 64 further comprising providing the devices in the virtual network with a communication agent.

66. (previously presented) The method of claim 65 wherein said providing the devices in the virtual network with a communication agent includes providing a proxy agent.

67. (canceled)

68. (previously presented) The method of claim 64 further comprising authenticating the devices as the members in the virtual network.

69. (previously presented) The method of claim 64 further comprising defining a member set of the virtual network that includes one or more of the devices, and assigning the domain name that defines the virtual network.

70. (previously presented) The method of claim 64 further comprising defining at least two member sets of the virtual network that each include one or more of the devices, the at least two member sets having at least one different device.

71. (previously presented) The method of claim 64 further comprising assigning the virtual network address to the device as an IPV4 compliant address.

72. (previously presented) The method of claim 71 wherein the IPV4 compliant address is non-routable.

73. (previously presented) The method of claim 64 further comprising routing network traffic via the public network from a first device having a public network address to a second device having a different public network address, the network traffic being routed as data packets having a source address which is the virtual network address of the first device and a destination address which is the virtual network address of the second device, the data packets being encapsulated to include a second source address which is a public network address of the first device and a second destination address which is the different public network address of the second device.

74. (previously presented) The method of claim 64 further comprising routing network traffic from a first device in a private physical network having a private network address to a second device having a public network address, the network traffic being routed as data packets having a source address which is the virtual network address of the first device, a destination address which is the virtual network address of the second device, and a shim which includes the private network address, the data packets being encapsulated to include a second destination address which is the public network address of the second device.

75. (previously presented) The method of claim 64 further comprising routing network traffic from a first device in a private physical network having a first private network address to a second device in a different private physical network having a second private network address, the network traffic being routed as encapsulated packets having a source address which is the virtual network address of the first device, a destination address which is the virtual network address of the second device, and a shim which includes the first and second private network addresses.

76. (previously presented) The method of claim 75 wherein the first private network address and the second private network address are identical.

77. (previously presented) The method of claim 64 further comprising responding to DNS requests received from the devices that are the members in the virtual network.

78. (previously presented) The method of claim 64 further comprising:

receiving a join status request from a first device in the virtual network as a query to determine the status of a second device in the virtual network; and

responding to the join status request to indicate whether or not the second device is joined to the virtual network for data communication.

79. (previously presented) The method of claim 64 further comprising applying a group policy to the devices that are registered as the members of the virtual network.

80. (currently amended) One or more processor readable storage media comprising processor readable code that, ~~when~~ if executed by a computer device, ~~initiates~~ implements a virtual network manager to:

receive registration requests from devices that request to be registered as members of a virtual network that is defined by a domain name having an associated public network address in a public network, each of the devices having an associated private network address; ~~and~~

distribute a virtual network address to a device to register the device as a member in the virtual network, each device in the virtual network being identified to the other devices by the virtual network address that is associated with the device; and

manage communications routed between the devices that are registered in the virtual network, the communications routed as encapsulated packets from a source device to a destination device, an encapsulated packet including a first virtual network address that corresponds to the source device and a second virtual network address that corresponds to the destination device.

81. (currently amended) One or more processor readable storage media as recited in claim 80 further comprising processor readable code that, ~~when~~ if executed, ~~initiates~~ implements the virtual network manager to provide the devices in the virtual network with a communication agent.

82. (previously presented) One or more processor readable storage media as recited in claim 81 wherein the virtual network manager provides the as a proxy agent.

83. (currently amended) One or more processor readable storage media as recited in claim 80 further comprising processor readable code that, ~~when~~ if executed, ~~initiates~~ implements the virtual network manager to define a member set of the virtual network that includes one or more of the devices, and the domain name that defines the virtual network.

84. (previously presented) One or more processor readable storage media as recited in claim 80 wherein the virtual network address includes a non-routable IPV4 compliant address.

85. (currently amended) One or more processor readable storage media as recited in claim 80 further comprising processor readable code that, ~~when~~ if executed, ~~initiates~~ implements the virtual network manager to route network traffic via the public network from a first device having a public network address to a second device having a different public network address.

86. (currently amended) One or more processor readable storage media as recited in claim 80 further comprising processor readable code that, ~~when~~ if executed, ~~initiates~~ implements the virtual network manager to route network traffic from a first device in a private physical network having a private network address to a second device having a public network address.

87. (currently amended) One or more processor readable storage media as recited in claim 80 further comprising processor readable code that, ~~when~~ if executed, ~~initiates~~ implements the virtual network manager to route network traffic from a first device in a private physical network having a first private network address to a second device in a different private physical network having a second private network address.

88. (previously presented) One or more processor readable storage media as recited in claim 87 wherein the network traffic is routed to the first or second device via a NAT device.

89. (previously presented) One or more processor readable storage media as recited in claim 87 wherein the first private network address and the second private network address are identical.

90. (previously presented) One or more processor readable storage media as recited in claim 85 wherein the network traffic is routed as encapsulated data packets.

91. (previously presented) One or more processor readable storage media as recited in claim 85 wherein the network traffic is routed as encrypted data traffic.

92. (currently amended) One or more processor readable storage media as recited in claim 80 further comprising processor readable code that, ~~when~~ if executed, ~~initiates~~ implements the virtual network manager to apply a group policy to the devices that are registered as the members of the virtual network.

93. (currently amended) A virtual network system, comprising:

a virtual network manager having a network interface coupled to a virtual network, the virtual network manager including at least one virtual community definition that is defined by a domain name having an associated public network address and a user set of one or more devices that are registered in the virtual network, each device in the virtual network being identified to the other devices by a virtual network address that is associated with the device, the virtual network manager configured to exchange virtual network information with the one or more devices of the user set, ~~and~~ the virtual network being accessible by devices in the user set and devices outside of the user set, and the virtual network manager further configured to receive a DNS request from a source device, and return a public network address of a route director, a private network address for a destination device, and a virtual network address that corresponds to the destination device.

94. (original) The system of claim 93 wherein the virtual network manager includes a member register module.

95. (original) The system of claim 93 wherein the virtual network manager includes a member join module.

96. (previously presented) The system of claim 95 wherein the member join module provides a virtual network address to a device that is registered as a member of the network.

97. (previously presented) The system of claim 93 wherein the virtual network manager is further configured to maintain data on an association between at least one virtual network address with at least one device that is registered as a member of the network.

98. (previously presented) The system of claim 93 wherein the virtual network manager includes a DNS server for the virtual community network.

99. (previously presented) The system of claim 93 wherein the virtual network manager includes a NAT device detector for devices connecting with the virtual network manager behind a NAT device.

100. (previously presented) The system of claim 93 wherein the virtual network manager includes at least a second virtual community definition.

101. (canceled)

102. (original) The system of claim 93 wherein the virtual network manager includes a member authenticator.

103. (previously presented) The system of claim 93 wherein the virtual network manager includes a DNS server configured to provide authoritative responses for DNS queries from devices in the virtual community.

104. (previously presented) The system of claim 93 further comprising at least one route director configured to communicate with the one or more devices in the user set.

105. (previously presented) The system of claim 93 wherein each device registered in the network is configured to communicate with the virtual network manager and other devices in the user set via at least one agent.

106. (previously presented) The system of claim 93 wherein the user set includes at least a first device and a second device, and wherein at least one of said first device and said second device is coupled to a first private network and accesses a public network via a NAT device.

107. (original) The system of claim 106 wherein said first device is coupled to said first private network, and said second device is coupled to a second private network and accesses the public network via a second NAT device.

108. (previously presented) The system of claim 93 wherein communications between the one or more devices in the user set are encrypted.

109. (previously presented) The system of claim 108 wherein the virtual network manager is configured to provide a shared message to the one or more devices in the user set to establish encrypted communications.

CLAIMS

We claim:

1. A virtual community network system, comprising:

a virtual network manager including at least one virtual community definition comprising at least a domain name and a user set; and

at least one route director capable of communicating with users in the user set.

2. The system of claim 1 wherein each user communicates with the virtual network manager and other users in the user set via at least one agent.

3. The system of claim 2 wherein the agent is installed on a processing device.

4. The system of claim 2 wherein the agent is installed on a proxy device.

5. The system of claim 2 wherein the virtual network manager includes a NAT device detector for agents installed on a processing device behind a NAT device.

6. The system of claim 1 wherein the manager comprises a device coupled to a public network and having a public network address.

7. The system of claim 1 wherein the user set includes at least a first user and a second user, said first user accesses other users in the community using at least a first processing device, said second user accesses other users in the community using at least a second processing device.

8. The system of claim 7 wherein each said device includes at least one virtual address in the community and at least one physical address.

9. The system of claim 8 wherein the physical address is dynamic.

10. The system of claim 8 wherein the physical address is static.

11. The system of claim 8 wherein the physical address is private.

12. The system of claim 8 wherein at least one of said first device or second device is coupled to a first private network and accesses a public network via a NAT device.

13. The system of claim 12 wherein the physical address is dynamic.

14. The system of claim 12 wherein the physical address is static.

15. The system of claim 12 wherein said first device is coupled to said first private network, and said second device is coupled to a second private network and accesses the public network via a second NAT device.

16. The system of claim 15 wherein said second device includes at least one virtual address in the realm and at least one private physical address.

17. The system of claim 15 wherein the physical address is dynamic.

18. The system of claim 15 wherein the physical address is static.

19. The system of claim 15 wherein said at least first private network and said at least second private network share at least one network address.

20. The system of claim 1 wherein the route director includes a pseudo address assignment for at least one user in the user set.

21. The system of claim 1 wherein the route director includes a translator for virtual address information for a virtual user in a private network realm.

22. The system of claim 1 wherein the virtual community manager is coupled to a public network and includes a public network address.

23. The system of claim 22 wherein the route director is coupled to said public network and includes a public network address.

24. The system of claim 22 wherein the route director is coupled to a first private network and said route director includes a private network address.

25. The system of claim 1 wherein communications between users in the user set are encapsulated.

26. The system of claim 1 wherein communications between users in the user set are encrypted.

27. The system of claim 26 wherein said encryption uses IPSEC.

28. The system of claim 26 wherein said encryption uses DES.

29. The system of claim 26 wherein said encryption uses triple DES.

30. The system of claim 1 wherein the manager includes at least a second virtual domain definition.

31. The system of claim 1 further including at least a first public route director and a second private route director.

32. A system, comprising:

a management device including network interface coupled to a public address realm and having a public address;

a virtual community network traffic router; and

router data including at least one association of a logical identifier with public routing information for a member.

33. The system of claim 32 wherein the network traffic router includes a network interface accessible by a public address in the public address realm.

34. The system of claim 32 wherein the management device includes a UDP port capable of receiving virtual community network traffic.

35. The system of claim 32 wherein the management device includes a TCP port capable of communicating virtual community network traffic.

36. The system of claim 32 wherein a member accesses a physical network via a processing device and the system further includes at least one agent installed on the processing device.

37. The system of claim 36 wherein the processing device is coupled to a private physical network behind a NAT device, and the network traffic router includes a transposer for routing information in a packet destined for the agent to direct the packet to the NAT device for the agent.

38. The system of claim 32 further including at least one proxy agent on a private physical network communicating with a member and the network traffic router.

39. The system of claim 38 wherein the member accesses other members using a device coupled to a private physical network.

40. The system of claim 32 wherein the manager includes a member register module.

41. The system of claim 40 wherein the manager includes a member join module.

42. The system of claim 41 wherein the join module provides a virtual address to a registered member.

43. The system of claim 41 wherein the manager maintains data on an association between at least one virtual address with at least one member.

44. The system of claim 40 wherein the manager includes a DNS server for the virtual community.

45. The system of claim 32 further including a virtual community network communication agent for a device, comprising a virtual network adapter interfacing with the device and applications on the device to route traffic to members of the virtual community via their virtual address.

46. The system of claim 45 wherein the agent includes a domain name routing plugin.

47. The system of claim 45 wherein the agent includes a separate IP stack for each user in the user set accessing the device.

48. The system of claim 45 wherein the adapter is a deterministic network enhancer.

49. The system of claim 45 wherein the adapter includes a DNS plugin.

50. The system of claim 45 wherein the adapter includes an IPSEC plugin.

51. The system of claim 45 wherein the adapter includes a domain name routing plugin.

52. The system of claim 45 wherein the agent includes a community registration module.

53. A virtual community network system, comprising:

a virtual community network manager;

a route director;

at least a first virtual community agent associated with a first community member; and

at least a second virtual community agent associated with at least a second community member.

54. The system of claim 53 wherein the route director is a network route director, and includes a public network interface and public address.

55. The system of claim 53 wherein the route director is a private route director, and includes a private physical network address interface and a private physical network address.

56. The system of claim 53 wherein the first or second virtual community network agent is installed on a device used by a member to access a network.

57. The system of claim 56 wherein the device is in a private physical network.

58. The system of claim 56 wherein the device is coupled to a public physical network.

59. The system of claim 53 wherein the first or second virtual community network agent is a proxy agent.

60. The system of claim 53 wherein the first and second members access the virtual community via devices coupled to separate private address physical realms.

61. The system of claim 53 wherein the virtual community network manager includes at least a first community definition and a second community definition.

62. The system of claim 53 wherein the community network manager includes a member authenticator.

63. The system of claim 62 wherein the community network manager includes a DNS server providing authorative responses for DNS queries in the virtual community.

64. A method for providing a secure virtual network, comprising:

providing a virtual network manager coupled to a public network;

defining a member set of users entitled to communicate in the virtual network;

registering members with the manager;

assigning members a virtual address; and

routing network traffic between the members in the virtual community.

65. The method of claim 64 further including the step of providing users in said member set with a communication agent.

66. The method of claim 65 wherein said step of providing users with a communication agent includes providing a proxy agent.

67. The method of claim 65 wherein said step of providing users with a communication agent includes providing an agent installed on a device used by the member to couple to a network.

68. The method of claim 65 wherein the step of registering comprises authenticating members with the member set.

69. The method of claim 64 wherein the step of defining a member set includes the step of assigning a domain name for the community.

70. The method of claim 64 wherein the step of defining a member set includes defining at least two member sets having at least one different member.

71. The method of claim 64 wherein the step of assigning a virtual address includes assigning an IPV4 compliant address.

72. The method of claim 71 wherein the step of assigning a virtual address includes assigning a non-routable IPV4 compliant address.

73. The method of claim 64 wherein the step of routing network traffic includes routing traffic from a first member accessing the public network on a first device having a public address with a second member accessing the public network on a second device having a different public address.

74. The method of claim 64 wherein the step of routing network traffic includes routing traffic from a first member accessing the public network on a first device in a private physical network having a private address with a second member accessing the public network on a second device having a public address.

75. The method of claim 64 wherein the step of routing network traffic includes routing traffic from a first member accessing the public network on a device in a private physical network having a first private physical address with a second member accessing the public network on a device in a private physical network having a second private physical address.

76. The method of claim 75 wherein the first private physical address and the second private physical address are identical.

77. The method of claim 64 further including the step of responding to DNS requests for members in the virtual network.

78. The method of claim 64 further including the step of responding to joined status requests for registered members in the virtual network.

79. The method of claim 64 further including applying a group policy to members of the virtual community.

80. One or more processor readable storage devices having processor readable code embodied on said processor readable storage devices, said processor readable code for programming one or more processors to perform a method comprising the steps of:

managing a virtual community network realm;

defining a member set of users entitled to communicate in the virtual community;

registering users with the virtual community;

assigning each user a virtual address; and

routing network traffic between the users in the virtual community.

81. One or more processor readable storage devices as defined in claim 80 further including code for programming one or more processors to perform a step of providing users in said member set with a communication agent.

82. One or more processor readable storage devices as defined in claim 81 wherein said step of providing users with a communication agent includes providing a proxy agent.

83 One or more processor readable storage devices as defined in claim 80 wherein the step of defining a member set includes the step of assigning a domain name for the community.

84. One or more processor readable storage devices as defined in claim 80 wherein the step of assigning a virtual address includes a non-routable IPV4 compliant address.

85. One or more processor readable storage devices as defined in claim 80 wherein the step of routing network traffic includes routing traffic from a first member accessing the public address realm on a first device having a public address with a second member accessing the public address realm on a second device having a different public address.

86. One or more processor readable storage devices as defined in claim 80 wherein the step of routing network traffic includes routing traffic from a first member accessing the public address realm on a first device in a private physical network having a private address with a second member accessing the public address realm on a second device having a public address.

87. One or more processor readable storage devices as defined in claim 80 wherein the step of routing network traffic includes routing traffic from a first member accessing the public address realm on a device in a private physical network having a first private physical address with a second member accessing the public address realm on a device in a private physical network having a second private physical address.

88. One or more processor readable storage devices as defined in claim 87 wherein the step of routing network traffic includes routing traffic to the first or second member via a NAT device.

89. One or more processor readable storage devices as defined in claim 87 wherein the first private physical address and the second private physical address are identical.

90. One or more processor readable storage devices as defined in claim 80 wherein the step of routing includes routing encapsulated traffic.

91. One or more processor readable storage devices as defined in claim 80 wherein the step of routing includes routing encrypted traffic.

92. One or more processor readable storage devices as defined in claim 80 further including applying a group policy to members of the virtual community.

93. A virtual community network system, comprising:

a virtual network manager having a network interface coupled to a network, the manager including at least one virtual community definition comprising at least a domain name and a user set, the network being assessable by users in the user set and users outside the user set, the manager exchanging virtual community network information with users in the user set.

94. The system of claim 93 wherein the virtual network manager includes a member register module.

95. The system of claim 93 wherein the virtual network manager includes a member join module.

96. The system of claim 95 wherein the join module provides a virtual address to a registered member.

97. The system of claim 93 wherein the virtual network manager maintains data on an association between at least one virtual address with at least one member.

98. The system of claim 93 wherein the virtual network manager includes a DNS server for the virtual community.

99. The system of claim 93 wherein the virtual network manager includes a NAT device detector for users connecting with the virtual network manager using a processing device behind a NAT device.

100. The system of claim 93 wherein the virtual network manager includes at least a second virtual domain definition.

101. The system of claim 93 wherein the virtual network manager includes at least a first virtual community definition and a second virtual community definition.

102. The system of claim 93 wherein the virtual network manager includes a member authenticator.

103. The system of claim 93 wherein the virtual network manager includes a DNS server providing authorative responses for DNS queries form users in the virtual community.

104. The system of claim 93 wherein the system further includes at least one route director capable of communicating with users in the user set.

105. The system of claim 93 wherein each user communicates with the virtual network manager and other users in the user set via at least one agent.

106. The system of claim 93 wherein the user set includes at least a first user and a second user, said first user accesses other users in the community using at least a first processing device, said second user accesses other users in the community using at least a second processing device, wherein at least one of said first device or second device is coupled to a first private network and accesses a public network via a NAT device.

107. The system of claim 106 wherein said first device is coupled to said first private network, and said second device is coupled to a second private network and accesses the public network via a second NAT device.

108. The system of claim 93 wherein communications between users in the user set are encrypted.

109. The system of claim 108 wherein the virtual network manager provides a shared secret to users in the user set to establish encrypted communications.